Notice of Allowability	Application No. 09/663,811	Applicant(s) HACHERL ET AL.	
	Examiner Shin-Hon Chen	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 10/30/06* .

2. ☒ The allowed claim(s) is/are *1,2,5-7,9-13 and 15-24*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11/15/06* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

CHRISTOPHER REVAK
PRIMARY EXAMINER

DETAILED ACTION

1. Claims 1, 2, 5-7, 9-13, and 15-24 are allowed. Claims 1, 2, 5-7, 9-13, and 15-24 are re-numbered as claims 1-20.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ryan Grace on 11/15/06.

The application has been amended as follows:

3. 1. (Currently amended) A computer-readable storage medium having computer-executable instructions for protecting network domain data against unauthorized modification in a distributed computer network having a plurality of network domains, comprising:

receiving, at a first computing machine, a request to modify an object associated with a shared data structure of a data store, wherein the data structure is replicated on ~~the shared data structure is shared by~~ the plurality of network domains, wherein the first computing machine resides in at least one of the network domains, wherein the object includes a security descriptor identifying an owner network domain of the object and an identification of at least one user, wherein the request includes at least one member of a group comprising: a fundamental modification and the security descriptor indicating a special security evaluation; ~~one or more users;~~

when the request includes a fundamental modification,

determining whether the first computing machine resides in the owner network domain by retrieving from the security descriptor the identity of the owner network domain and comparing the owner network domain identity to the network domain within which the first computing machine resides; ~~and~~

rejecting the request to modify the object when the first computing machine does not reside in the owner network domain[.]; and

when the request includes the security descriptor indicating the special security evaluation,

sending a notification to the first computing machine that a security evaluation is to be evaluated within the owner network domain.

4. 2. (Currently amended) The computer-readable storage medium of claim 1, further comprising, allowing the request to modify the object when the first computing machine resides in the owner network domain.

5. 3. (Cancelled)

6. 5. (Currently amended) The computer-readable storage medium of claim 1, wherein the security descriptor further comprises a field that indicates ~~whether a~~ that the special security evaluation should be performed on requests to modify the object.~~, and wherein the computer-~~

~~executable instructions further comprise, causing the special security evaluation to be performed when the field indicates that the special security evaluation should be performed.~~

7. 6. (Currently amended) The computer-readable storage medium of claim 5, wherein the special security evaluation comprises requesting that a second computing machine within the owner network domain evaluate whether an entity issuing the request to modify the object is authorized to modify the object.

8. 7. (Currently amended) A computer-implemented method for protecting network domain data against unauthorized modification in a distributed computer network having a plurality of network domains, comprising:

receiving, from a requester at a first machine in a first network domain in the plurality of network domains, a request to modify an object, wherein the object is associated with a shared data structure replicated on the plurality of network domains, the request including a security token identifying at least one group of which the requester is a member, the object having an associated security descriptor identifying an owner network domain of the object and having an identification of at least one user ~~one or more users~~, the object having a flag to identify whether a special security evaluation is to be performed on requests to modify the object;

determining from the flag whether the special security evaluation is to be performed on the request to modify the object;

when the flag indicates that the special security evaluation is to be performed, performing the special security evaluation on the request to modify the object when the flag indicates in the

affirmative, wherein the special security evaluation on the request to modify the object is performed by passing the security token associated with the request and the security descriptor associated with the object to the owner network domain for evaluation[;], and allowing the request to modify the object to proceed when the special security evaluation approves the request to modify the object[.];

when the flag indicates that the special security evaluation is not to be performed, performing a security evaluation on the first network domain.

9. 9. (Currently amended) The ~~computer-readable medium~~ computer-implemented method of claim 7, further comprising, performing a security evaluation on the request to modify the object when the flag indicates in the negative.

10. 10. (Currently amended) The ~~computer-readable medium~~ computer-implemented method of claim 9, wherein the security evaluation comprises comparing the security token with the security descriptor to determine whether the requester is a member of any group that have been granted permission to access the object.

11. 11. (Currently amended) The ~~computer-readable medium~~ computer-implemented method of claim 10,wherein the security evaluation further comprises determining whether the request to modify the object is a modification for which the requester is privileged on the first machine regardless of whether the requester is a member of any groups that have been granted permission to access the object.

12. 12. (Currently amended) The ~~computer-readable medium~~ computer-implemented method of claim 11, wherein the security evaluation further comprises denying the request when the requester is privileged to perform the request to modify the object, the requested modification is a fundamental modification of the object, and the first network domain is not the owner network domain of the object.

13. 13. (Currently amended) A computer-readable storage medium having computer-executable components to protect network domain data against unauthorized modification in a distributed computer network having a plurality of network domains; comprising:

a shared data structure of the plurality of domains, at least two network domains in the plurality of network domains having a transitive trust relationship wherein a user authentication within one of the two network domains is honored in the other of the two network domains, the shared data structure having at least one data store that is replicated among each of the plurality of network domains;

an object stored within the data store, the object having a plurality of attributes, at least one of the attributes being related to security access rights associated with the object, the security access rights including an owner network domain identifier identifying one of the domains within the plurality of domains, an indicator configured to indicate that an attempt to access the object is to be evaluated within the network domain identified by the owner network domain, and an identification of at least one user ~~one or more users~~; and

a security system configured to receive a request to modify the object, to determine from the indicator whether the request to modify the object should be evaluated within the network domain identified by the owner, and when so, to return a notification to the requestor that the security evaluation is to be evaluated within the network domain identified by the owner network domain, to retrieve from the object the owner network domain identifier, to compare the owner network domain identifier with an identifier of a network domain from which the request originated, and to reject the request to modify the object if the owner network domain identifier does not match the identifier of the network domain from which the request originated.

14. 14. (Cancelled)

15. 15. (Currently amended) The computer-readable storage medium of claim [14] 13, wherein the notification to the requestor comprises a referral message including an identification of the owner network domain.

16. 16. (Currently amended) The computer-readable storage medium of claim 13, wherein the security system is further configured to determine whether the request to modify the object originated within a particular network domain of the plurality of network domains, and when ~~if~~ so, perform a standard security evaluation of the request to modify the object without resort to the owner network domain.

17. 17. (Currently amended) The computer-readable storage medium of claim 16, wherein the particular network domain is a root network domain of the shared data structure.

18. 18. (Currently amended) The computer-readable storage medium of claim 13, wherein the shared data structure comprises a directory service and wherein the at least one data store comprises configuration data associated with the directory service.

19. 19. (Currently amended) The computer-readable storage medium of claim 13, wherein the shared data structure comprises a directory service and wherein the at least one data store comprises schema data associated with the directory service.

20. 20. (Currently amended) The computer-readable storage medium of claim 13, wherein the at least one attribute comprises a security descriptor and permissions associated with the at least one user ~~one or more users~~, and the owner network domain identifier is part of an owner security identifier.

21. 21. (Currently amended) The computer-readable storage medium of claim 1, wherein the security descriptor includes permissions associated with the at least one user ~~one or more users~~.

22. 22. (Currently amended) The ~~computer-readable medium~~ computer-implemented method of claim 7, wherein the security descriptor includes permissions associated with the at least one user ~~one or more users~~.

23. 23. (New) The computer-implemented method of claim 7, wherein the request to modify the object includes a request to make a fundamental change.

24. 24. (New) The computer-readable storage medium of claim 13, wherein the request to modify the object includes a request to make a fundamental change.

Allowable Subject Matter

25. The following is an examiner's statement of reasons for allowance: The prior art of record discloses multi-domain access control that manages access control to resources that belong to multiple domains governed by an access control system and the access is granted to a user when the user obtains access control cookie required to access resources in another domain. However, the closest prior art of record individually or in combination does not explicitly disclose a data structure that is replicated on the plurality of network domains; a security descriptor indicating a special security evaluation; sending a notification to the first computing machine that a security evaluation is to be evaluated within the owner network domain when the security descriptor indicating the special security evaluation in light of other features disclosed in independent claims 1, 7, and 13.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

CHRISTOPHER REVAK
PRIMARY EXAMINER